

This Page Is Inserted by IFW Operations
and is not a part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

**As rescanning documents *will not* correct images,
please do not report the images to the
Image Problem Mailbox.**



1 / 1

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-148742
 (43)Date of publication of application : 30.05.2000

(51)Int.CI. G06F 17/21

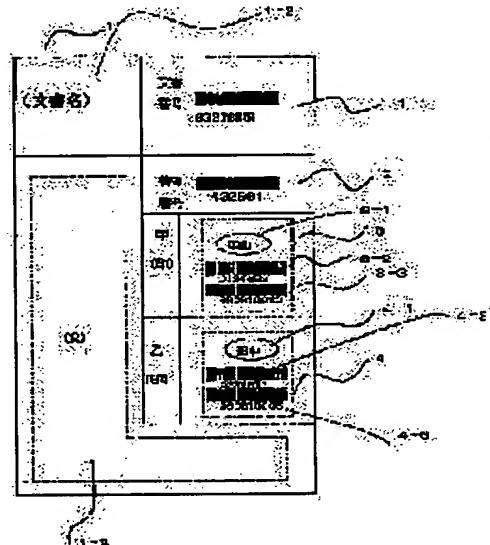
(21)Application number : 10-336474 (71)Applicant : NEC CORP
 (22)Date of filing : 12.11.1998 (72)Inventor : HIROSE TAKASHI

(54) SYSTEM AND METHOD FOR AUTHENTICATION MANAGEMENT

(57)Abstract:

PROBLEM TO BE SOLVED: To make it easy to confirm whether a seal or a signature image is genuine by adding a management number as a basis for authentication in a bar code form to a seal of authentication included in the print result of an electronic document and adding the code of a storage system in a bar code form to the electronic document.

SOLUTION: Electronic document data 1 are saved in an electronic document data storage system, and the management number specifying the system and its bar code 2, the document management number and its bar code 1-1, and authentication data 3 and 4 of an authenticator are presented in the document. Thus, the management number and use numbers 3-3 and 4-3 as a basis for the authentication of a seal or a signature image are added in a bar code form in a phase where it is easily confirmed whether or not the seal or signature image are genuine, the management number of the document and the code of the storage system are added in a bar code form in the print document, and the resultant electronic document is saved.



LEGAL STATUS

[Date of request for examination] 12.11.1998

[Date of sending the examiner's decision of rejection] 08.07.2003

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

*** NOTICES ***

Japan Patent Office is not responsible for any damages caused by the use of this translation.

1. This document has been translated by computer. So the translation may not reflect the original precisely.
- 2.**** shows the word which can not be translated.
3. In the drawings, any words are not translated.

Bibliography

(19) [Country of Issue] Japan Patent Office (JP)
(12) [Official Gazette Type] Open patent official report (A)
(11) [Publication No.] JP,2000-148742,A (P2000-148742A)
(43) [Date of Publication] May 30, Heisei 12 (2000. 5.30)
(54) [Title of the Invention] An authentication managerial system and an authentication management method
(51) [The 7th edition of International Patent Classification]

G06F 17/21

[FI]

G06F 15/20 570 M
570 R

[Request for Examination] Tamotsu
[The number of claims] 14
[Mode of Application] FD
[Number of Pages] 10
(21) [Filing Number] Japanese Patent Application No. 10-336474
(22) [Filing Date] November 12, Heisei 10 (1998. 11.12)
(71) [Applicant]
[Identification Number] 000004237
[Name] NEC Corp.
[Address] 5-7-1, Shiba, Minato-ku, Tokyo
(72) [Inventor(s)]
[Name] Hirose **
[Address] 5-7-1, Shiba, Minato-ku, Tokyo Inside of NEC Corp.
(74) [Attorney]
[Identification Number] 100097113
[Patent Attorney]
[Name] Ditch ****
[Theme code (reference)]

5B009

[F term (reference)]

5B009 SA11 SA14

[Translation done.]

* NOTICES *

Japan Patent Office is not responsible for any damages caused by the use of this translation.

1. This document has been translated by computer. So the translation may not reflect the original precisely.
- 2.**** shows the word which can not be translated.
3. In the drawings, any words are not translated.

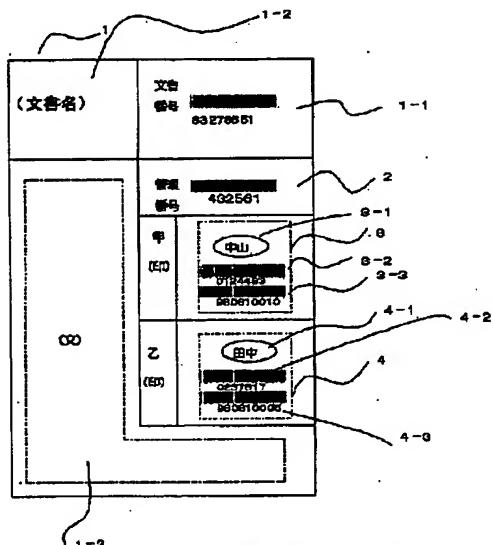
Summary

(57) [Abstract]

[Technical problem] The check of the truth or falsehood of authentication is easy for this invention, and it makes it a technical problem to offer an authentication managerial system and an authentication management method with opening and reliability.

[Means for Solution] While the check of the seal as authentication or the truth or falsehood of a sign image displays by the bar code that the management number and the operating number of the authentication are easy the seal as authentication, and near the sign image, the management number of a document and a storage engine's code are displayed by the bar code into a printing document. And it is open, and it sets to the electronic text data storage system which keeps an electronic text file for realization of a reliable authentication managerial system and an authentication management method, and the authentication data storage system which keeps image datas, such as a seal of an individual or a corporation, and a sign, as authentication data, and the management number and text management number of authentication data are kept and managed mutually.

[Translation done.]



1—電子文書データ
 1—1…文書管理の文書番号とそのバーコード
 1—2…文書名
 1—3…文
 2…管理番号とそのバーコード
 3, 4…認証者の認証データ
 3—1, 4—1…認証イメージデータ
 3—2, 4—2…管理番号と認証者の管理番号
 3—3, 4—3…使用番号

[Translation done.]

* NOTICES *

Japan Patent Office is not responsible for any damages caused by the use of this translation.

1. This document has been translated by computer. So the translation may not reflect the original precisely.
- 2.**** shows the word which can not be translated.
3. In the drawings, any words are not translated.

CLAIMS

[Claim(s)]

[Claim 1] The authentication managerial system of the electronic filing document which used the computer etc. characterized by providing the following A means to append the basis of the authentication concerned, the management number which can change, and/or an operating number in bar code form to the seal and/or sign image as authentication which are displayed on the printing result of the electronic filing document and/or electronic filing document which used the computer etc. A means to write in addition the code of the basis of the authentication to a document, the management number which can change, and/or a storage system in bar code form into the electronic filing document concerned

[Claim 2] The authentication managerial system of the electronic filing document which used the computer etc. characterized by providing the following The electronic text data storage system keep the electronic filing document which used the computer etc. in the state at the time of registration of recognition data with the management number of the basis of the authentication to the basis of the authentication to the text recognition person of the electronic filing document concerned, the authentication data which can change, and the text recognition person concerned, and the authentication data which can change, and generate the electronic text data added the authentication data based on the electronic text management number which can change with the basis of the authentication to the The authentication data storage system which sends the basis of the authentication to the authentication data which kept the basis of the authentication to an individual or a corporation, and image datas which can change, such as a seal and a sign, as authentication data, and had the demand concerned according to the demand from an individual and a corporation concerned, and the authentication data concerned, and the management number which can change to the aforementioned electronic text data storage system

[Claim 3] The authentication managerial system of the electronic filing document which used the computer etc. characterized by providing the following The electronic text data storage system which writes the management number of a document, and/or a storage engine's code in addition in bar code form into a printing document, and keeps in the aforementioned electronic filing document while writing in addition the management number and/or the operating number which are the seal as an authentication means, and/or near the sign image, and can change with the basis of the authentication to the seal concerned and/or a sign image in the position where the check of the truth or falsehood of the seal concerned and/or a sign image is easy in bar code form The basis of the authentication to an individual and/or a corporation, and the seal and sign which can change

[Claim 4] The aforementioned electronic text data storage system is an authentication managerial system according to claim 2 or 3 characterized by having the function which transmits and receives the aforementioned electronic text data safely from the user by whom the connected aforementioned computer system was specified.

[Claim 5] The aforementioned electronic text data storage system is an authentication managerial system given in the claim 2 characterized by keeping the aforementioned electronic text data, reading a required authentication person from the electronic text data concerned, obtaining the approval of an authentication person using means of communications, and having the function to receive the aforementioned authentication data from the aforementioned authentication data storage system, or any 1 term of 4.

[Claim 6] The aforementioned authentication data storage system is an authentication managerial system given in the claim 2 characterized by having the function which carries out storage management of the aforementioned authentication data received from the authentication person, or any 1 term of 5.

[Claim 7] The aforementioned authentication data storage system is an authentication managerial system according to claim 6 characterized by having the function to take recognition by an authentication person's computer system and means of communications, and to send the aforementioned authentication data with a management number, corresponding to the authentication data demand from the aforementioned electronic text data acquired through a network between the aforementioned electronic text data storage systems.

[Claim 8] The authentication management method of the electronic filing document which used the computer etc. characterized by providing the following The process which appends the basis of the authentication concerned, the management number which can change, and/or an operating number in bar code form to the seal and/or sign image as authentication which are displayed on the printing result of the electronic filing document and/or electronic filing document which used the computer etc. The process which writes in addition the code of the basis of the authentication to a document, the management number which can change, and/or a storage system in bar code form into the electronic filing document concerned

[Claim 9] The authentication management method of the electronic filing document which used the computer etc. characterized by providing the following The electronic text data storage process of keeping the electronic filing document which used the computer etc. in the state at the time of registration of recognition data with the management number of the basis of the authentication to the basis of the authentication to the text recognition person of the electronic filing document concerned, the authentication data which can change, and the text recognition person concerned, and the authentication data which can change, and generating the electronic text data added the authentication data based on the electronic text management number which can change with the basis of the authentication to The authentication data storage process of sending the basis of the authentication to the authentication data which kept the basis of the authentication to an individual or a corporation, and image datas which can change, such as a seal and a sign, as authentication data, and had the demand concerned according to the demand from an individual and a corporation concerned, and the authentication data concerned, and the management number which can change to the aforementioned electronic text data storage process

[Claim 10] The authentication management method of the electronic filing document which used the computer etc. characterized by providing the following The electronic text data storage process which writes the management number of a document, and/or a storage engine's code in addition in bar code form into a printing document, and keeps in the aforementioned electronic filing document while writing in addition the management number and/or the operating number which is the seal as an authentication process, and/or near the sign image, and can change with the basis of the authentication to the seal concerned and/or a sign image in the position where the check of the truth or falsehood of the seal concerned and/or a sign image is easy in bar code form The basis of the authentication to an individual and/or a corporation, and the seal and sign which can change

[Claim 11] The aforementioned electronic text data storage process is an authentication management method according to claim 9 or 10 characterized by having the process which transmits and receives the aforementioned electronic text data safely from the user by whom the connected aforementioned computer system was specified.

[Claim 12] The aforementioned electronic text data storage process is an authentication

management method given in the claim 9 characterized by keeping the aforementioned electronic text data, reading a required authentication person from the electronic text data concerned, obtaining the approval of an authentication person using a communication process, and having the process which receives the aforementioned authentication data from the aforementioned authentication data storage process, or any 1 term of 11.

[Claim 13] The aforementioned authentication data storage process is an authentication management method given in the claim 9 characterized by having the process which carries out storage management of the aforementioned authentication data received from the authentication person, or any 1 term of 12.

[Claim 14] The aforementioned authentication data storage process is an authentication management method according to claim 13 characterized by having the process which takes recognition according to an authentication person's computer system and communication process, and sends the aforementioned authentication data with a management number corresponding to the authentication data demand from the aforementioned electronic text data acquired through a network between the aforementioned electronic text data storage processes.

[Translation done.]

* NOTICES *

Japan Patent Office is not responsible for any damages caused by the use of this translation.

1. This document has been translated by computer. So the translation may not reflect the original precisely.
- 2.**** shows the word which can not be translated.
3. In the drawings, any words are not translated.

DETAILED DESCRIPTION

[Detailed Description of the Invention]

[0001]

[The technical field to which invention belongs] Especially this invention relates to the authentication managerial system and authentication management method of an electronic filing document of computer use about authentication technology.

[0002]

[Description of the Prior Art] In recent years, printing and means of displaying with the easy check of the seal as authentication or the truth or falsehood of a sign image displayed on the printing result of the electronic filing document and electronic filing document which used the computer etc. are called for, and authentication data and an electronic filing document -- each -- separate -- and -- relating -- a check -- it is rich in the open nature which utilized keeping it with an easy gestalt, and the network, and the reliable authentication managerial system and the authentication management method are searched for

[0003] As the authentication managerial system and authentication management method of an electronic filing document of such computer use, the technology of a publication is indicated by JP,6-119363,A, for example (the conventional technology). In the electronic-filing-document recognition method of a computer system with which the electronic-filing-document recognition method of the conventional technology treats a word processor and the document of an E-mail A document data-storage means to memorize the created electronic-filing-document data, and a recognition image means to memorize by making seal and sign of a recognition person into an image data corresponding to a recognition person number, A store protection attribute addition

means to add the store protection attribute which makes improper a data change of the electronic-filing-document data memorized by the document data-storage means to the electronic-filing-document data, The recognition information addition means to which add the recognition information which contains a recognition person number in the electronic-filing-document data memorized by the document data-storage means by operation of a recognition person, and a store protection attribute is made to add through a store protection attribute addition means, The electronic-filing-document data with which the recognition information addition means which the document data-storage means has memorized added recognition information and the store protection attribute are read by specification of a recognition person number. It is constituted by having a synthetic output means to compound to the electronic-filing-document data which read the image data corresponding to the recognition person number memorized for the recognition image-data storage means, and to output to an output unit. Furthermore, it sets to recognition of the electronic filing document of the word processor by the computer, or an E-mail. The result which can make a change of document data improper having a recognition image data, compounding and outputting at the time of an output, and by adding recognition information to document data by operation of a recognition person, The unjust recognition by human being without the qualification to recognize can be prevented, and the unjust change after recognition can be prevented, and it is said that it is effective in the ability to protect an electronic filing document from the intentional action by the malice of human beings, such as a crime and a malfeasance.

[0004]

[Problem(s) to be Solved by the Invention] However, only by the printed authentication data division, since the check of authentication data was not easy, the conventional technology had the trouble that the judgment of the truth or falsehood of the authentication data was difficult.

[0005] Furthermore, since the independent system environment is not built and a text data control number is not sent to an authentication data storage system, each operating number is not memorized by the printed authentication data. Consequently, each text data could not be searched from authentication data, but there was also a trouble that neither text management nor authentication data control could be performed as an open system.

[0006] while printing and a display with the easy check of the seal as authentication or the truth or falsehood of a sign image displayed on the printing result of the electronic filing document and the electronic filing document which used the computer etc. can perform the place which this invention is made in view of this trouble, and makes into the purpose -- authentication data and an electronic filing document -- each -- separate -- and -- relating -- a check -- it is to the point of it being rich in the open nature which can keep with an easy gestalt, and offering a reliable authentication

[0007]

[Means for Solving the Problem] The summary of this invention is the authentication managerial system of the electronic filing document which used the computer etc. With the seal and/or sign image as authentication which are displayed on the printing result of the electronic filing document and/or electronic filing document which used the computer etc. A means to write in addition the basis of the authentication concerned, the management number which can change, and/or an operating number in bar code form, It consists in the authentication managerial system characterized by having a means to write in addition the code of the basis of the authentication to a document, the management number which can change, and/or a storage system in bar code form into the electronic filing document concerned. Moreover, the summary of this invention according to claim 2 is the authentication managerial system of the electronic filing document which used the computer etc. The electronic filing document which used the computer etc. is kept in the state at the time of registration of recognition data with the management number of the basis of the authentication to the basis of the authentication to the text recognition person of the electronic filing document concerned, the authentication data which can change, and the text recognition person concerned, and the authentication data which can change. The basis of the authentication to the aforementioned electronic filing document, and the electronic text data storage system which generates the electronic text data to which

the authentication data based on the electronic text management number which can change were added. The basis of the authentication to an individual or a corporation and image datas which can change, such as a seal and a sign, are kept as authentication data. It consists in the authentication managerial system characterized by having the basis of the authentication to authentication data with the demand concerned, and the authentication data concerned, and the authentication data storage system which sends the management number which can change to the aforementioned electronic text data storage system according to the demand from an individual and a corporation concerned. Moreover, the summary of this invention according to claim 3 is the authentication managerial system of the electronic filing document which used the computer etc. It is the seal as an authentication means, and/or near the sign image. in an easy position, the check of the truth or falsehood of the seal concerned and/or a sign image While writing in addition the basis of the authentication to the seal concerned and/or a sign image, the management number which can change, and/or an operating number in bar code form The electronic text data storage system which writes the management number of a document, and/or a storage engine's code in addition in bar code form into a printing document, and keeps the aforementioned electronic filing document, It has the basis of the authentication to an individual and/or a corporation, and the authentication data storage system which keeps an image data including the seal which can change, or a sign as authentication data. The aforementioned electronic text data storage system and the aforementioned authentication data storage system consist in the authentication managerial system characterized by keeping and managing the management number and text management number of the aforementioned authentication data mutually. Moreover, it consists in the authentication managerial system according to claim 2 or 3 characterized by the summary of this invention according to claim 4 having the function which transmits and receives the aforementioned electronic text data safely from the user by whom the aforementioned computer system to which the aforementioned electronic text data storage system was connected was specified. Moreover, the aforementioned electronic text data storage system keeps the aforementioned electronic text data, and reads a required authentication person from the electronic text data concerned, the summary of this invention according to claim 5 obtains the approval of an authentication person using means of communications, and it consists to an authentication managerial system given in the claim 2 characterized by having the function to receive the aforementioned authentication data from the aforementioned authentication data storage system, or any 1 term of 4. Moreover, it consists in an authentication managerial system given in the claim 2 characterized by the summary of this invention according to claim 6 having the function which carries out storage management of the aforementioned authentication data which received the aforementioned authentication data storage system from the authentication person, or any 1 term of 5. Moreover, corresponding to the authentication data demand from the aforementioned electronic text data acquired through a network between the aforementioned electronic text data storage systems, the summary of this invention according to claim 7 takes recognition by an authentication person's computer system and means of communications, and the aforementioned authentication data storage system consists in it to the authentication managerial system according to claim 6 characterized by having the function to send the aforementioned authentication data with a management number. Moreover, the summary of this invention according to claim 8 is the authentication management method of the electronic filing document which used the computer etc. With the seal and/or sign image as authentication which are displayed on the printing result of the electronic filing document and/or electronic filing document which used the computer etc. The process which writes in addition the basis of the authentication concerned, the management number which can change, and/or an operating number in bar code form, It consists in the authentication management method characterized by having the process which writes in addition the code of the basis of the authentication to a document, the management number which can change, and/or a storage system in bar code form into the electronic filing document concerned. Moreover, the summary of this invention according to claim 9 is the authentication management method of the electronic filing document which used the computer etc. The electronic filing document which used the computer etc. is kept in the state at the time of registration of

recognition data with the management number of the basis of the authentication to the basis of the authentication to the text recognition person of the electronic filing document concerned, the authentication data which can change, and the text recognition person concerned, and the authentication data which can change. The basis of the authentication to the aforementioned electronic filing document, and the electronic text data storage process which generates the electronic text data to which the authentication data based on the electronic text management number which can change were added. The basis of the authentication to an individual or a corporation and image datas which can change, such as a seal and a sign, are kept as authentication data. It consists in the authentication management method characterized by having the basis of the authentication to authentication data with the demand concerned, and the authentication data concerned, and the authentication data storage process of sending the management number which can change to the aforementioned electronic text data storage process, according to the demand from an individual and a corporation concerned. Moreover, the summary of this invention according to claim 10 is the authentication management method of the electronic filing document which used the computer etc. It is the seal as an authentication process, and/or near the sign image. in an easy position, the check of the truth or falsehood of the seal concerned and/or a sign image While writing in addition the basis of the authentication to the seal concerned and/or a sign image, the management number which can change, and/or an operating number in bar code form The electronic text data storage process of writing the management number of a document, and/or a storage engine's code in addition in bar code form into a printing document, and keeping the aforementioned electronic filing document, It has the basis of the authentication to an individual and/or a corporation, and the authentication data storage process of keeping an image data including the seal which can change, or a sign as authentication data. The aforementioned electronic text data storage process and the aforementioned authentication data storage process are ** about keeping and managing the management number and text management number of the aforementioned authentication data mutually. It consists in the authentication management method considered as the mark. Moreover, it consists in the authentication management method according to claim 9 or 10 characterized by the summary of this invention according to claim 11 having the process at which the aforementioned electronic text data storage process transmits from the user by whom the connected aforementioned computer system was specified and receives the aforementioned electronic text data safely. Moreover, the aforementioned electronic text data storage process keeps the aforementioned electronic text data, and reads a required authentication person from the electronic text data concerned, the summary of this invention according to claim 12 obtains the approval of an authentication person using a communication process, and it consists to an authentication management method given in the claim 9 characterized by having the process which receives the aforementioned authentication data from the aforementioned authentication data storage process, or any 1 term of 11. Moreover, it consists in an authentication management method given in the claim 9 characterized by the summary of this invention according to claim 13 having the process which carries out storage management of the aforementioned authentication data which received the aforementioned authentication data storage process from the authentication person, or any 1 term of 12. Moreover, corresponding to the authentication data demand from the aforementioned electronic text data storage processes, the summary of this invention according to claim 14 takes recognition according to an authentication person's computer system and communication process, and the aforementioned authentication data storage process consists in it, to the authentication management method according to claim 13 characterized by to have the process which sends the aforementioned authentication data with a management number.

[0008]

[Embodiments of the Invention] Hereafter, the gestalt of operation of this invention is explained in detail based on a drawing.

[0009] (The 1st operation gestalt) Drawing 1 is the functional block diagram showing 1 operation gestalt of the authentication managerial system of this invention. As shown in drawing 1, the

authentication managerial system of this operation gestalt has mutually arbitrary numbers of electronic text data storage systems 20 connected possible [communication] safely, and arbitrary numbers of authentication data storage systems 30 and 40 on arbitrary numbers of computer systems 10 and 50 which had safety mutually and were connected to it possible [communication] in the network 60, and the network 60.

[0010] Computer systems 10 and 50 have the output function to print image datas, such as communication facility which performs transmission and reception of the electronic text data 1 by means of communications with safeties, such as a word processor function, a password, etc. which create the electronic text data 1, an authentication function to perform transmission and reception of the authentication data 3 and 4, and a bar code.

[0011] The electronic text data storage system 20 of this operation gestalt are a means to perform an electronic text data storage process, and the electronic filing document which used the computer etc. It is kept in the state at the time of registration of recognition data with the management number of the basis of the authentication to the basis of the authentication to the text recognition person of this electronic filing document, the authentication data which can change, and this text recognition person, and the authentication data which can change. The electronic text data 1 to which the authentication data based on the basis of the authentication to an electronic filing document and the electronic text management number which can change were added are generated.

[0012] If it puts in another way, the electronic text data storage system 20 It is the seal as an authentication means, and/or near the sign image. in an easy position, the check of the truth or falsehood of this seal and/or a sign image While writing in addition the basis of the authentication to this seal and/or a sign image, the management number which can change and/or the operating number 3-3, and 4-3 in bar code form The management number of a document and/or a storage engine's code are written in addition in bar code form into a printing document, and an electronic filing document is kept.

[0013] Moreover, the electronic text data storage system 20 keeps the function which transmits and receives the electronic text data 1 safely from the user by whom the connected computer systems 10 and 50 were specified, and the electronic text data 1, reads a required authentication person from the electronic text data 1, obtains the approval of an authentication person using means of communications, and has the function to receive the authentication data 3 and 4 from the authentication data storage systems 30 and 40.

[0014] The authentication data storage systems 30 and 40 of this operation form are means to perform an authentication data storage process, keep the basis of the authentication to an individual or a corporation, and image datas which can change, such as a seal and a sign, as authentication data, and send authentication data with this demand and the basis of the authentication to this authentication data, and the management number it can change to the electronic text data storage system 20 according to the demand from this individual and corporation.

[0015] If it puts in another way, the authentication data storage systems 30 and 40 will keep an image data including the basis of the authentication to an individual and/or a corporation, the seal which can change, or a sign as authentication data 3 and 4.

[0016] Such the electronic text data storage system 20 and the authentication data storage systems 30 and 40 keep and manage the management number and text management number of the authentication data 3 and 4 mutually.

[0017] Moreover, while the authentication data storage systems 30 and 40 carry out storage management of the authentication data 3 and 4 received from the authentication person, corresponding to the authentication data demand from the electronic text data 1 acquired through a network 60 between the electronic text data storage systems 20, they take recognition by an authentication person's computer systems 10 and 50 and means of communications, and have the function to send the authentication data 3 and 4 with a management number.

[0018] Then, operation of the authentication managerial system of this operation gestalt is explained.

[0019] The electronic text data 1 are created using a computer system 10, and if their recognition data are appended and kept to the electronic text data storage system 20, according to storage of this recognition data, the electronic text data storage system 20 will require a required authentication person's authentication data 3 and 4 of the authentication data storage systems 30 and 40.

[0020] According to a demand, each authentication data storage systems 30 and 40 receive these authentication data 3 and 4, temporary storage of the electronic text data storage system 20 to the document data control number is carried out, the approval of each authentication person is obtained, and the authentication data 3 and 4 and a management number are sent to the electronic text data storage system 20.

[0021] According to sending of these authentication data 3 and 4 and a management number, the authentication data storage systems 30 and 40 keep a document data control number.

[0022] According to this, the electronic text data storage system 20 fills in the management number and the management number of the electronic text data storage system 20 as the authentication data 3 and 4 into an electronic filing document after collecting each authentication data 3 and 4, displays the management number in a bar code, keeps it as electronic text data 1, and transmits the electronic text data 1 to each authentication person's computer systems 10 and 50.

[0023] According to transmission of this electronic text data 1, each received computer systems 10 and 50 print by keeping the electronic text data 1.

[0024] Next, in the authentication managerial system of this operation gestalt, process in which the electronic text data 1 shown in drawing 2 were created is explained. Drawing 2 shows the outline composition of the printing result of the electronic text data 1 used with the authentication managerial system of drawing 1.

[0025] The electronic text data 1 shown in drawing 2 are kept by the electronic text data storage system 20, and it has in the document the management number which specifies the system, publication number and bar code 1-1 of the bar code 2 and a documentation management, and an authentication person's authentication data 3 and 4. Moreover, a title is indicated in the place of the document name 1-2, and the content of a sentence is indicated by the electronic text data 1 in the place of a sentence 1-3.

[0026] The authentication data 3 have the authentication image data 3-1, the management number of the authentication data storage system 30 and an authentication person's management number 3-2, the operating numbers 3-3, and these bar codes in each.

[0027] The authentication data 4 have the authentication image data 4-1, the management number of the authentication data storage system 40 and an authentication person's management number 4-2, the operating numbers 4-3, and these bar codes in each.

[0028] Drawing 3 is a flow chart which shows 1 operation gestalt of the document preparation procedure which used the authentication management method of this invention. The authentication management method of this operation gestalt is an authentication management method of the electronic filing document which used the computer etc. With the seal and/or sign image as authentication which are displayed on the printing result of the electronic filing document and/or electronic filing document which used the computer etc. The process which writes in addition the basis of this authentication, the management number which can change, and/or an operating number in bar code form, In order to perform the process which writes in addition the code of the basis of the authentication to a document, the management number which can change, and/or a storage system in bar code form into this electronic filing document, it has the electronic text data storage process and the authentication data storage process.

[0029] An electronic text data storage process is a process which the electronic text data storage system 20 performs, as shown in drawing 3. The electronic filing document which used the computer etc. is kept in the state at the time of registration of recognition data with the management number of the basis of the authentication to the basis of the authentication to the text recognition person of this electronic filing document, the authentication data which can change, and this text recognition person, and the authentication data which can change. The electronic text data 1 to which the authentication data based on the basis of the authentication

to an electronic filing document and the electronic text management number which can change were added are generated.

[0030] If it puts in another way, an electronic text data storage process will be the seal as an authentication process, and/or near the sign image. the check of the truth or falsehood of this seal and/or a sign image in an easy position While writing in addition the basis of the authentication to this seal and/or a sign image, the management number which can change and/or the operating number 3-3, and 4-3 in bar code form The management number of a document and/or a storage engine's code are written in addition in bar code form into a printing document, and an electronic filing document is kept.

[0031] Such an electronic text data storage process has the process which transmits and receives the electronic text data 1 safely from the user by whom the connected computer systems 10 and 50 were specified, it keeps the electronic text data 1, reads a required authentication person from this electronic text data 1, obtains the approval of an authentication person using a communication process, and has the process which receives the authentication data 3 and 4 from an authentication data storage process.

[0032] On the other hand, as an authentication data storage process is shown in drawing 3, it is the process which the authentication data storage systems 30 and 40 perform, and the basis of the authentication to an individual or a corporation and image datas which can change, such as a seal and a sign, are kept as authentication data, and authentication data with this demand and the basis of the authentication to this authentication data, and the management number it can change are sent to an electronic text data storage process according to the demand from this individual and corporation

[0033] If it puts in another way, an authentication data storage process will keep an image data including the basis of the authentication to an individual and/or a corporation, the seal which can change, or a sign as authentication data 3 and 4.

[0034] Such an electronic text data storage process and an authentication data storage process keep and manage the management number and text management number of the authentication data 3 and 4 mutually.

[0035] Such an authentication data storage process has the process which carries out storage management of the authentication data 3 and 4 received from the authentication person, corresponding to the authentication data demand from the electronic text data 1 acquired through a network 60 between electronic text data storage processes, takes recognition according to an authentication person's computer systems 10 and 50 and communication process, and has the process send the authentication data 3 and 4 with a management number.

[0036] Next, the creation procedure of the electronic text data 1 is explained using drawing 3. It is the case of the first which the electronic text data 1 show to drawing 2, and the documents (a contract etc. is included) which two persons of the second recognize, and "first" ("Mr. Nakayama" who shows drawing 2 and drawing 3) which is one of authentication persons uses a computer system 10, and explains the case which creates the electronic text data 1.

[0037] " -- Mr. Nakayama" creates the spurious data of the electronic text to which an authentication person's authentication management number was attached using the computer system 10. Here, a spurious data is called because the management number of the electronic text data storage system 20, a publication number, and the authentication data 3 and 4 are not included yet.

[0038] A computer system 10 acquires a documentation-management number from this electronic text data storage system 20 while transmitting the spurious data of this electronic text to the electronic text data storage system 20.

[0039] The electronic text data storage system 20 carries out temporary storage of the acquired documentation-management number at the documentation-management file 21.

[0040] The electronic text data storage system 20 requires the authentication data 3 and 4 of each of the authentication data storage systems 30 and 40 based on the authentication management number of the required authentication person in the electronic text data 1. When requiring the authentication data 3 and 4 of each of the authentication data storage systems 30 and 40, the electronic text data storage system 20 transmits the management number, the

documentation-management number, and the temporary electronic text data 1 of a system. [0041] Demand sequence is searched for based on a maker's authentication data 3 and 4. Each authentication data storage systems 30 and 40 of which the authentication data 3 and 4 were required append the temporary document of the electronic text data 1, and ask each authentication person for recognition.

[0042] According to approval of Mr. Nakayama", the authentication data 3 come to hand from the authentication data storage system 30, and the electronic text data storage system 20 receives the authentication data 4 from the authentication data storage system 40 by ["correspond to first" " through the authentication data storage system 30 / "correspond to second" " through the authentication data storage system 40] obtaining the approval of Mr. Tanaka."

[0043] Each authentication data storage systems 30 and 40 are made to correspond to each authentication person's management number currently kept by each of the authentication management files 31 and 41, and associate and keep the operating number 3-3, 4-3 and the management number of the electronic text data storage system 20, and the management number of a document.

[0044] The authentication data 3 have the authentication image data 3-1, the management number of the authentication data storage system 30 and an authentication person's management number 3-2, the operating numbers 3-3, and these bar codes in each.

[0045] The authentication data 4 have the authentication image data 4-1, the management number of the authentication data storage system 40 and an authentication person's management number 4-2, the operating numbers 4-3, and these bar codes in each.

[0046] The electronic text data storage system 20 completes the final electronic text data 1, and keeps them to the documentation-management file 21 in the state where it was protected.

[0047] It becomes able [the specific man or the specific ordinary men who were permitted] to receive and print the electronic text data 1 by accessing this electronic text data storage system 20 from computer systems 10 and 50 to check the contents of this electronic text data 1.

[0048] If the 1st operation form is summarized above The check of the seal as authentication and/or the truth or falsehood of a sign image so that easily While writing in addition the basis of the authentication, the management number which can change and/or the operating number 3-3, and 4-3 in a number and bar code form near the seal as authentication, and/or the sign image By writing the management number of a document, and/or a storage engine's code in addition in a number and bar code form into a printing document, and checking by the computer systems 10 and 50 with a bar code reader The authentication data 3 and 4 and the electronic text data 1 can be searched quickly, and it can take out now from each storage system. Consequently, the authentication data storage systems 30 and 40 can be easily deduced from the authentication data 3 and 4 contained in the electronic text data 1, and the truth or falsehood of the authentication data 3 and 4 can be easily judged by accessing, and it has the merit of being easy to search the electronic text data 1.

[0049] Furthermore An image data including the basis of the authentication to the electronic text data storage system 20 and individual who keep the electronic text data 1 which need the authentication data 3 and 4, and/or a corporation, the seal which can change, or a sign as authentication data 3 and 4 By constituting the authentication data storage systems 30 and 40 to keep as an independent system, and connecting this to an authentication person's computer systems 10 and 50 and the authentication data storage system 30, and both 40 in a network 60 The maker of the electronic text data 1 the created temporary electronic text data 1 once It is kept to the electronic text data storage system 20, and while the electronic text data storage system 20 obtains the authentication data 3 and 4 through the authentication data storage systems 30 and 40, the management number and text management number of the authentication data 3 and 4 can be kept and managed mutually. Consequently, the electronic text data storage system 20 and the authentication data storage systems 30 and 40 are the system which became independent respectively, and can constitute now the open system which was rich in safety.

[0050] (The 2nd operation form) As for the authentication managerial system of this operation

form, a maker does temporary acquisition of his authentication data 3 and 4 from the authentication data storage systems 30 and 40 at the time of creation of the spurious data of an electronic text. At this time, the management number or text number of the electronic text data storage system 20 are not given to the authentication data storage systems 30 and 40, but the temporary use number of the authentication data 3 and 4 is transmitted to them.

[0051] Transmission of a management number or a publication number is performed between the electronic text data storage system 20, the authentication data storage system 30, and 40, without obtaining the approval of a maker, after temporary text data are transmitted to the electronic text data storage system 20. In this case, it has the merit that a part of recognition procedure can reduce a labor.

[0052] If the 2nd operation form is summarized above The check of the seal as authentication and/or the truth or falsehood of a sign image so that easily While writing in addition the basis of the authentication, the management number which can change and/or the operating number 3-3, and 4-3 in a number and bar code form near the seal as authentication, and/or the sign image By writing the management number of a document, and/or a storage engine's code in addition in a number and bar code form into a printing document, and checking by the computer systems 10 and 50 with a bar code reader The authentication data 3 and 4 and the electronic text data 1 can be searched quickly, and it can take out now from each storage system. Consequently, the authentication data storage systems 30 and 40 can be easily deduced from the authentication data 3 and 4 contained in the electronic text data 1, and the truth or falsehood of the authentication data 3 and 4 can be easily judged by accessing, and it has the merit of being easy to search the electronic text data 1.

[0053] Furthermore An image data including the basis of the authentication to the electronic text data storage system 20 and individual who keep the electronic text data 1 which need the authentication data 3 and 4, and/or a corporation, the seal which can change, or a sign as authentication data 3 and 4 The authentication data storage systems 30 and 40 to keep are constituted as an independent system. this in a network 60 An authentication person's computer systems 10 and 50, And by connecting the authentication data storage systems 30 and 40 mutually The maker of the electronic text data 1 the created temporary electronic text data 1 once It is kept to the electronic text data storage system 20, and while the electronic text data storage system 20 obtains the authentication data 3 and 4 through the authentication data storage systems 30 and 40, the management number and text management number of the authentication data 3 and 4 can be kept and managed mutually. Consequently, the electronic text data storage system 20 and the authentication data storage systems 30 and 40 are the system which became independent respectively, and can constitute now the open system which was rich in safety.

[0054] In addition, this invention is not limited to electronic text data, but when applying this invention, in the gestalt of this operation, it is widely applicable to the authentication technology over suitable cybermoney (Electronic Money, Digital Cash), the authentication technology over a credit card, the authentication technology over electronic commerce (electronic commerce : Electronic Commerce), the authentication technology over an electronic banking system (electronic banking : Electronic Banking), etc. moreover, the above-mentioned composition -- the number of members, a position, a configuration, etc. are not limited to the gestalt of the above-mentioned implementation, but when carrying out this invention, they can be made into a suitable number, a position, a configuration, etc. Moreover, in each drawing, the same sign is given to the same component.

[0055]

[Effect of the Invention] this invention While the check of the seal as authentication or the truth or falsehood of a sign image writes the management number and the operating number of the authentication with it being easy in addition in bar code form the seal as authentication, and near the sign image, the management number of a document and a storage engine's code are written in addition in bar code form into a printing document. In the electronic text data storage system which is rich in open nature and keeps an electronic filing document for realization of a reliable authentication managerial system and an authentication management method, and the

authentication data storage system which keeps image datas, such as a seal of an individual or a corporation, and a sign, as authentication data. The management number and text management number of authentication data are kept and managed mutually.

[0056] The check of whether to have recognized the text data from the authentication data storage system can be taken now by reading the bar code under authentication data using the bar code reader of the computer connected to the managerial system of both an electronic text data storage system and an authentication data storage system in communication by this.

Moreover, the bar code of the management number of text data is read, and the text can check the right thing from an electronic text data storage system. Consequently, it comes to be able to perform printing and a display with the easy check of the seal as authentication, or the truth or falsehood of a sign image displayed on the printing result of the electronic filing document and electronic filing document which used the computer etc., and the effect that improvement in security nature can be aimed at is done so.

[0057] Moreover, the effect that the check of the seal as authentication or the truth or falsehood of a sign image displayed on the printing result of an electronic filing document and an electronic filing document becomes easy is done so by adding the bar code of a management number to authentication data.

[0058] furthermore, the thing mutually done for storage management while attaching a management number to authentication data and text data -- authentication data and an electronic filing document -- each -- separate -- and -- relating -- a check -- it can be kept now with an easy gestalt. Consequently, the effect that it is compatible in high reliability with high open nature is done so.

[Translation done.]

* NOTICES *

Japan Patent Office is not responsible for any damages caused by the use of this translation.

1. This document has been translated by computer. So the translation may not reflect the original precisely.
- 2.**** shows the word which can not be translated.
3. In the drawings, any words are not translated.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]

[Drawing 1] It is the functional block diagram showing 1 operation gestalt of the authentication managerial system of this invention.

[Drawing 2] The outline composition of the printing result of the electronic text data used with the authentication managerial system of drawing 1 is shown.

[Drawing 3] It is the flow chart which shows 1 operation gestalt of the document preparation procedure using the authentication management method of this invention.

[Description of Notations]

- 1 -- Electronic text data
- 1-1 -- The publication number and its bar code of a documentation management
- 1-2 -- Document name
- 1-3 -- Sentence
- 2 -- A management number and its bar code
- 3 4 -- An authentication person's authentication data
- 3-1, 4-1 -- Authentication image data

3-2, 4-2 — A management number and an authentication person's management number
3-3, 4-3 — Operating number
10 50 — Computer system
20 — Electronic text data storage system
21 — Documentation-management file
30 40 — Authentication data storage system
31 41 — Authentication management file
60 — Network

[Translation done.]

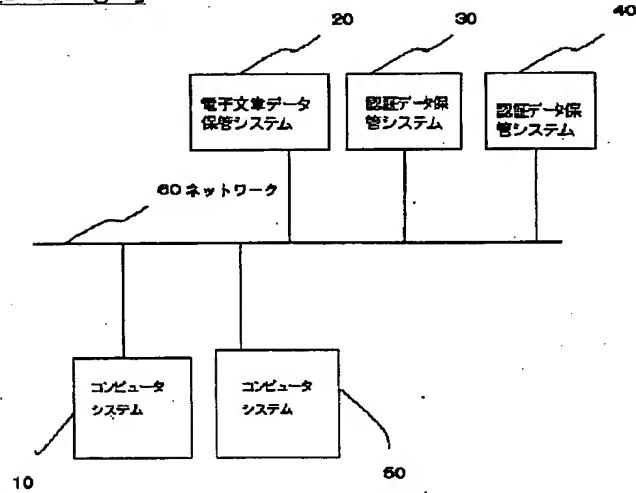
* NOTICES *

Japan Patent Office is not responsible for any damages caused by the use of this translation.

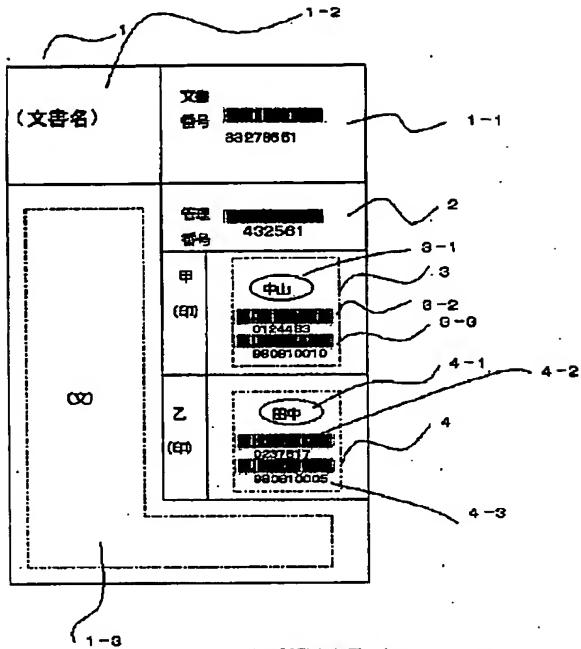
1. This document has been translated by computer. So the translation may not reflect the original precisely.
- 2.**** shows the word which can not be translated.
3. In the drawings, any words are not translated.

DRAWINGS

[Drawing 1]

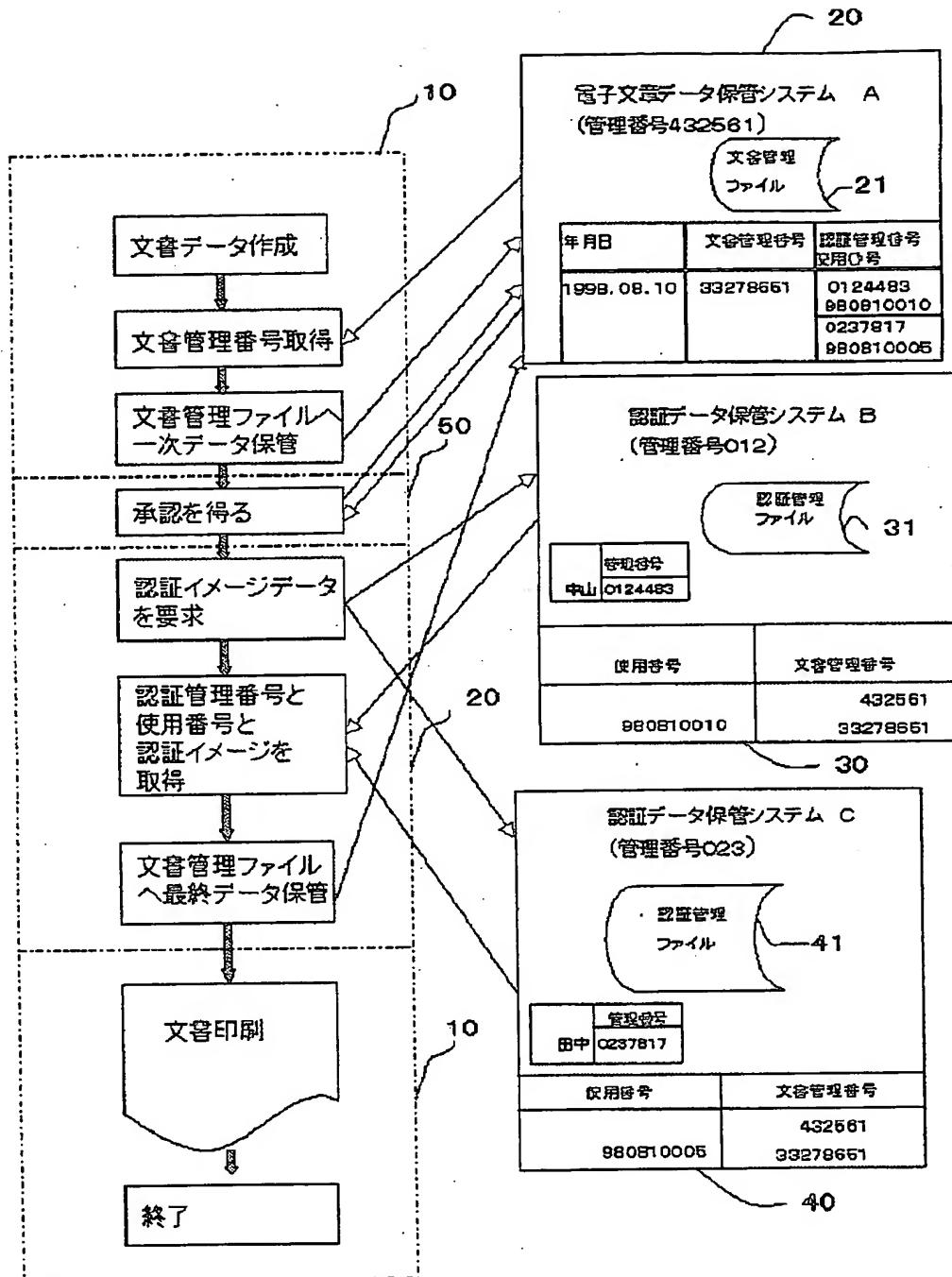


[Drawing 2]



1…電子文章データ
 1-1…文書管理の文書番号とそのバーコード
 1-2…文書名
 1-3…文
 2…管理番号とそのバーコード
 3, 4…認証者の認証データ
 3-1, 4-1…認証イメージデータ
 3-2, 4-2…管理番号と認証者の管理番号
 3-3, 4-3…使用番号

[Drawing 3]



[Translation done.]

(19) 日本国特許庁 (JP)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2000-148742

(P2000-148742A)

(43) 公開日 平成12年5月30日 (2000.5.30)

(51) Int.Cl.

G 0 6 F 17/21

識別記号

F I

テーマコード (参考)

G 0 6 F 15/20

5 7 0 M 5 B 0 0 9

5 7 0 R

審査請求 有 請求項の数14 FD (全 10 頁)

(21) 出願番号 特願平10-336474

(71) 出願人 000004237

日本電気株式会社

東京都港区芝五丁目7番1号

(22) 出願日 平成10年11月12日 (1998.11.12)

(72) 発明者 広瀬 隆

東京都港区芝五丁目7番1号 日本電気株式会社内

(74) 代理人 100097113

弁理士 堀 城之

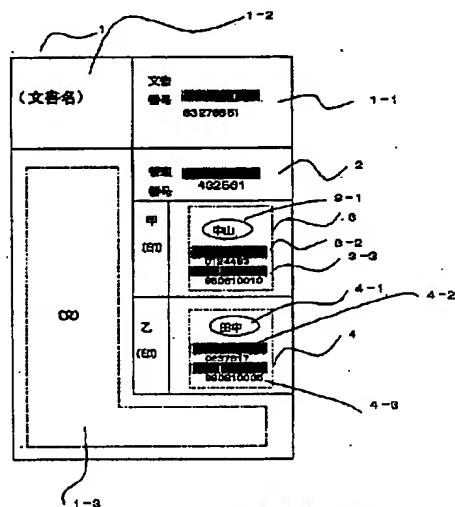
F ターム (参考) 5B009 SA11 SA14

(54) 【発明の名称】 認証管理システム及び認証管理方法

(57) 【要約】

【課題】 本発明は、認証の真偽の確認が容易でオープンかつ信頼性のある認証管理システム及び認証管理方法を提供することを課題とする。

【解決手段】 認証としての印章やサインイメージの真偽の確認が容易なように認証としての印章やサインイメージの近傍にその認証の管理番号及び使用番号をバーコードで表示するとともに印字文書の中に文書の管理番号、及び保管機関のコードをバーコードで表示する。そしてオープンで信頼性のある認証管理システム及び認証管理方法の実現のため電子文章ファイルを保管する電子文章データ保管システムと個人や法人の印章やサインなどのイメージデータを認証データとして保管する認証データ保管システムにおいて、相互に認証データの管理番号と文章管理番号を保管及び管理する。



- 1-電子文書データ
- 1-1-文書管理の文書番号とそのバーコード
- 1-2-文書名
- 1-3-文
- 2-認証番号とそのバーコード
- 3, 4-認証者の認証データ
- 3-1, 4-1-認証イメージデータ
- 3-2, 4-2-認証番号と認証者の管理番号
- 3-3, 4-3-使用番号

【特許請求の範囲】

【請求項1】 コンピュータ等を使用した電子文書の認証管理システムであって、コンピュータ等を使用した電子文書及び／または電子文書の印字結果に表示される認証としての印章及び／またはサインイメージに、当該認証の根拠と成り得る管理番号及び／または使用番号をバーコード形式で付記する手段と、文書に対する認証の根拠と成り得る管理番号及び／または保管システムのコードを当該電子文書中にバーコード形式で付記する手段とを有することを特徴とする認証管理システム。

【請求項2】 コンピュータ等を使用した電子文書の認証管理システムであって、コンピュータ等を使用した電子文書を、当該電子文書の文章承認者に対する認証の根拠と成り得る認証データ及び当該文章承認者に対する認証の根拠と成り得る認証データの管理番号とともに承認データの受付時の状態で保管し、前記電子文書に対する認証の根拠と成り得る電子文章管理番号に基づく認証データを追加した電子文章データを生成する電子文章データ保管システムと、個人や法人に対する認証の根拠と成り得る印章やサインなどのイメージデータを認証データとして保管し、当該個人や法人からの要求に応じて、当該要求のあった認証データ及び当該認証データに対する認証の根拠と成り得る管理番号を前記電子文章データ保管システムに送付する認証データ保管システムとを有することを特徴とする認証管理システム。

【請求項3】 コンピュータ等を使用した電子文書の認証管理システムであって、認証手段としての印章及び／またはサインイメージの近傍であって当該印章及び／またはサインイメージの真贋の確認が容易な位置に、当該印章及び／またはサインイメージに対する認証の根拠と成り得る管理番号及び／または使用番号をバーコード形式で付記するとともに、印字文書の中に文書の管理番号及び／または保管機関のコードをバーコード形式で付記して前記電子文書を保管する電子文章データ保管システムと、個人及び／または法人に対する認証の根拠と成り得る印章やサインを含むイメージデータを認証データとして保管する認証データ保管システムとを有し、前記電子文章データ保管システムと前記認証データ保管システムとは、相互に前記認証データの管理番号と文章管理番号を保管及び管理することを特徴とする認証管理システム。

【請求項4】 前記電子文章データ保管システムは、接続された前記コンピュータシステムの特定されたユーザーから前記電子文章データを安全に送受信する機能を有することを特徴とする請求項2または3に記載の認証管理システム。

【請求項5】 前記電子文章データ保管システムは、前記電子文章データを保管し、当該電子文章データから必要な認証者を読み出し、通信手段を用いて認証者の承認を得て、前記認証データ保管システムから前記認証データを受け取る機能を有することを特徴とする請求項2乃至4のいずれか一項に記載の認証管理システム。

【請求項6】 前記認証データ保管システムは、認証者から受け取った前記認証データを保管管理する機能を有することを特徴とする請求項2乃至5のいずれか一項に記載の認証管理システム。

【請求項7】 前記認証データ保管システムは、前記電子文章データ保管システムとの間でネットワークを介して取得する前記電子文章データからの認証データ要求に対応して、認証者のコンピュータシステムと通信手段により承認を取り、管理番号付きの前記認証データを送付する機能を有することを特徴とする請求項6に記載の認証管理システム。

【請求項8】 コンピュータ等を使用した電子文書の認証管理方法であって、コンピュータ等を使用した電子文書及び／または電子文書の印字結果に表示される認証としての印章及び／またはサインイメージに、当該認証の根拠と成り得る管理番号及び／または使用番号をバーコード形式で付記する工程と、文書に対する認証の根拠と成り得る管理番号及び／または保管システムのコードを当該電子文書中にバーコード形式で付記する工程とを有することを特徴とする認証管理方法。

【請求項9】 コンピュータ等を使用した電子文書の認証管理方法であって、コンピュータ等を使用した電子文書を、当該電子文書の文章承認者に対する認証の根拠と成り得る認証データ及び当該文章承認者に対する認証の根拠と成り得る認証データの管理番号とともに承認データの受付時の状態で保管し、前記電子文書に対する認証の根拠と成り得る電子文章管理番号に基づく認証データを追加した電子文章データを生成する電子文章データ保管工程と、個人や法人に対する認証の根拠と成り得る印章やサインなどのイメージデータを認証データとして保管し、当該個人や法人からの要求に応じて、当該要求のあった認証データ及び当該認証データに対する認証の根拠と成り得る管理番号を前記電子文章データ保管工程に送付する認証データ保管工程とを有することを特徴とする認証管理方法。

【請求項10】 コンピュータ等を使用した電子文書の認証管理方法であって、認証工程としての印章及び／またはサインイメージの近傍であって当該印章及び／またはサインイメージの真贋の確認が容易な位置に、当該印章及び／またはサインイメージに対する認証の根拠と成り得る管理番号及び／または使用番号をバーコード形式で付記して前記電子文書を保管する電子文章データ保管システムと、個人及び／または法人に対する認証の根拠と成り得る印章やサインを含むイメージデータを認証データとして保管する認証データ保管システムとを有し、前記電子文章データ保管システムと前記認証データ保管システムとは、相互に前記認証データの管理番号と文章管理番号を保管及び管理することを特徴とする認証管理方法。

たは使用番号をバーコード形式で付記するとともに、印字文書の中に文書の管理番号及び／または保管機関のコードをバーコード形式で付記して前記電子文書を保管する電子文章データ保管工程と、

個人及び／または法人に対する認証の根拠と成り得る印章やサインを含むイメージデータを認証データとして保管する認証データ保管工程とを有し、

前記電子文章データ保管工程と前記認証データ保管工程とは、相互に前記認証データの管理番号と文章管理番号を保管及び管理することを特徴とする認証管理方法。

【請求項11】前記電子文章データ保管工程は、接続された前記コンピュータシステムの特定されたユーザーから前記電子文章データを安全に送受信する工程を有することを特徴とする請求項9または10に記載の認証管理方法。

【請求項12】前記電子文章データ保管工程は、前記電子文章データを保管し、当該電子文章データから必要な認証者を読み出し、通信工程を用いて認証者の承認を得て、前記認証データ保管工程から前記認証データを受け取る工程を有することを特徴とする請求項9乃至11のいずれか一項に記載の認証管理方法。

【請求項13】前記認証データ保管工程は、認証者から受け取った前記認証データを保管管理する工程を有することを特徴とする請求項9乃至12のいずれか一項に記載の認証管理方法。

【請求項14】前記認証データ保管工程は、前記電子文章データ保管工程との間でネットワークを介して取得する前記電子文章データからの認証データ要求に対応して、認証者のコンピュータシステムと通信工程とにより承認を取り、管理番号付きの前記認証データを送付する工程を有することを特徴とする請求項13に記載の認証管理方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、認証技術に関し、特に、コンピュータ使用の電子文書の認証管理システム及び認証管理方法に関する。

【0002】

【従来の技術】近年、コンピュータ等を使用した電子文書及び電子文書の印字結果に表示される認証としての印章やサインイメージの真贋の確認が容易な印字及び表示方式が求められている。そして、認証データと電子文書を各々別々にかつ関連づけて、確認容易な形態で保管すること、ネットワークを活用したオープン性に富みかつ信頼性の高い認証管理システム及び認証管理方法が求められている。

【0003】このようなコンピュータ使用の電子文書の認証管理システム及び認証管理方法としては、例えば、特開平6-119363号公報に記載の技術が開示されている（従来技術）。従来技術の電子文書承認方式は、

ワードプロセッサや電子メールの文書を扱うコンピュータシステムの電子文書承認方式において、作成された電子文書データを記憶する文書データ記憶手段と、承認者の印章やサインをイメージデータとして承認者番号と対応して記憶する承認イメージ手段と、文書データ記憶手段に記憶されている電子文書データのデータ変更を不可とする書込み保護属性をその電子文書データに付加する書込み保護属性付加手段と、承認者の操作により文書データ記憶手段に記憶されている電子文書データに承認者番号を含む承認情報を付加し、書込み保護属性付加手段を介して書込み保護属性を付加させる承認情報付加手段と、文書データ記憶手段が記憶している承認情報付加手段が承認情報および書込み保護属性を付加した電子文書データを承認者番号の指定により読み出し、承認イメージデータ記憶手段に記憶している承認者番号に対応するイメージデータを読み出した電子文書データに合成して出力装置に出力する合成出力手段とを有することにより構成される。更に、コンピュータによるワードプロセッサや電子メールの電子文書の承認において、承認イメージデータを持ち、出力時に合成して出力すること、および承認者の操作により文書データに承認情報を付加することにより文書データの変更を不可とすることができる結果、承認する資格のない人間による不正な承認を防ぐことができ、また、承認後の不正な変更を防ぐことができ、電子文書を、犯罪、不正行為などの人間の悪意による意図的行為から保護することができる効果があることが述べられている。

【0004】

【発明が解決しようとする課題】しかしながら、従来技術は、印字された認証データ部だけでは認証データの確認が容易ではないため、その認証データの真贋の判定が困難であるという問題点があった。

【0005】更に、独立したシステム環境が構築されておらず、認証データ保管システムに文章データ管理番号が送られないため、印字された認証データに個々の使用番号が記憶されない。その結果、認証データから個々の文章データを検索できず、オープンなシステムとして文章管理や認証データ管理ができないという問題点もあった。

【0006】本発明は斯かる問題点を鑑みてなされたものであり、その目的とするところは、コンピュータ等を使用した電子文書及び電子文書の印字結果に表示される認証としての印章やサインイメージの真贋の確認が容易な印字及び表示ができるとともに、認証データと電子文書を各々別々にかつ関連づけて確認容易な形態で保管できるオープン性に富みかつ信頼性の高い認証管理システム及び認証管理方法を提供する点にある。

【0007】

【課題を解決するための手段】本発明の要旨は、コンピュータ等を使用した電子文書の認証管理システムであつ

て、コンピュータ等を使用した電子文書及び／または電子文書の印字結果に表示される認証としての印章及び／またはサインイメージに、当該認証の根拠と成り得る管理番号及び／または使用番号をバーコード形式で付記する手段と、文書に対する認証の根拠と成り得る管理番号及び／または保管システムのコードを当該電子文書中にバーコード形式で付記する手段とを有することを特徴とする認証管理システムに存する。また本発明の請求項2に記載の要旨は、コンピュータ等を使用した電子文書の認証管理システムであって、コンピュータ等を使用した電子文書を、当該電子文書の文章承認者に対する認証の根拠と成り得る認証データ及び当該文章承認者に対する認証の根拠と成り得る認証データの管理番号とともに承認データの受付時の状態で保管し、前記電子文書に対する認証の根拠と成り得る電子文章管理番号に基づく認証データを追加した電子文章データを生成する電子文章データ保管システムと、個人や法人に対する認証の根拠と成り得る印章やサインなどのイメージデータを認証データとして保管し、当該個人や法人からの要求に応じて、当該要求のあった認証データ及び当該認証データに対する認証の根拠と成り得る管理番号を前記電子文章データ保管システムに送付する認証データ保管システムとを有することを特徴とする認証管理システムに存する。また本発明の請求項3に記載の要旨は、コンピュータ等を使用した電子文書の認証管理システムであって、認証手段としての印章及び／またはサインイメージの近傍であって当該印章及び／またはサインイメージの真質の確認が容易な位置に、当該印章及び／またはサインイメージに対する認証の根拠と成り得る管理番号及び／または使用番号をバーコード形式で付記するとともに、印字文書の中に文書の管理番号及び／または保管機関のコードをバーコード形式で付記して前記電子文書を保管する電子文章データ保管システムと、個人及び／または法人に対する認証の根拠と成り得る印章やサインを含むイメージデータを認証データとして保管する認証データ保管システムとを有し、前記電子文章データ保管システムと前記認証データ保管システムとは、相互に前記認証データの管理番号と文章管理番号を保管及び管理することを特徴とする認証管理システムに存する。また本発明の請求項4に記載の要旨は、前記電子文章データ保管システムは、接続された前記コンピュータシステムの特定されたユーザーから前記電子文章データを安全に送受信する機能を有することを特徴とする請求項2または3に記載の認証管理システムに存する。また本発明の請求項5に記載の要旨は、前記電子文章データ保管システムは、前記電子文章データを保管し、当該電子文章データから必要な認証者を読み出し、通信手段を用いて認証者の承認を得て、前記認証データ保管システムから前記認証データを受け取る機能を有することを特徴とする請求項2乃至4のいずれか一項に記載の認証管理システムに存する。ま

た本発明の請求項6に記載の要旨は、前記認証データ保管システムは、認証者から受け取った前記認証データを保管管理する機能を有することを特徴とする請求項2乃至5のいずれか一項に記載の認証管理システムに存する。また本発明の請求項7に記載の要旨は、前記認証データ保管システムは、前記電子文章データ保管システムとの間でネットワークを介して取得する前記電子文章データからの認証データ要求に対応して、認証者のコンピュータシステムと通信手段とにより承認を取り、管理番号付きの前記認証データを送付する機能を有することを特徴とする請求項6に記載の認証管理システムに存する。また本発明の請求項8に記載の要旨は、コンピュータ等を使用した電子文書の認証管理方法であって、コンピュータ等を使用した電子文書及び／または電子文書の印字結果に表示される認証としての印章及び／またはサインイメージに、当該認証の根拠と成り得る管理番号及び／または使用番号をバーコード形式で付記する工程と、文書に対する認証の根拠と成り得る管理番号及び／または保管システムのコードを当該電子文書中にバーコード形式で付記する工程とを有することを特徴とする認証管理方法に存する。また本発明の請求項9に記載の要旨は、コンピュータ等を使用した電子文書の認証管理方法であって、コンピュータ等を使用した電子文書を、当該電子文書の文章承認者に対する認証の根拠と成り得る認証データ及び当該文章承認者に対する認証の根拠と成り得る認証データの管理番号とともに承認データの受付時の状態で保管し、前記電子文書に対する認証の根拠と成り得る電子文章管理番号に基づく認証データを追加した電子文章データを生成する電子文章データ保管工程と、個人や法人に対する認証の根拠と成り得る印章やサインなどのイメージデータを認証データとして保管し、当該個人や法人からの要求に応じて、当該要求のあった認証データ及び当該認証データに対する認証の根拠と成り得る管理番号を前記電子文章データ保管工程に送付する認証データ保管工程とを有することを特徴とする認証管理方法に存する。また本発明の請求項10に記載の要旨は、コンピュータ等を使用した電子文書の認証管理方法であって、認証工程としての印章及び／またはサインイメージの近傍であって当該印章及び／またはサインイメージの真質の確認が容易な位置に、当該印章及び／またはサインイメージに対する認証の根拠と成り得る管理番号及び／または使用番号をバーコード形式で付記するとともに、印字文書の中に文書の管理番号及び／または保管機関のコードをバーコード形式で付記して前記電子文書を保管する電子文章データ保管工程と、個人及び／または法人に対する認証の根拠と成り得る印章やサインを含むイメージデータを認証データとして保管する認証データ保管工程とを有し、前記電子文章データ保管工程と前記認証データ保管工程とは、相互に前記認証データの管理番号と文章管理番号を保管及び管理することを特

徴とする認証管理方法に存する。また本発明の請求項1に記載の要旨は、前記電子文章データ保管工程は、接続された前記コンピュータシステムの特定されたユーザーから前記電子文章データを安全に送受信する工程を有することを特徴とする請求項9または10に記載の認証管理方法に存する。また本発明の請求項12に記載の要旨は、前記電子文章データ保管工程は、前記電子文章データを保管し、当該電子文章データから必要な認証者を読み出し、通信工程を用いて認証者の承認を得て、前記認証データ保管工程から前記認証データを受け取る工程を有することを特徴とする請求項9乃至11のいずれか一項に記載の認証管理方法に存する。また本発明の請求項13に記載の要旨は、前記認証データ保管工程は、認証者から受け取った前記認証データを保管管理する工程を有することを特徴とする請求項9乃至12のいずれか一項に記載の認証管理方法に存する。また本発明の請求項14に記載の要旨は、前記認証データ保管工程は、前記電子文章データ保管工程との間でネットワークを介して取得する前記電子文章データからの認証データ要求に対応して、認証者のコンピュータシステムと通信工程により承認を取り、管理番号付きの前記認証データを送付する工程を有することを特徴とする請求項13に記載の認証管理方法に存する。

【0008】

【発明の実施の形態】以下、本発明の実施の形態を図面に基づいて詳細に説明する。

【0009】(第1実施形態)図1は、本発明の認証管理システムの一実施形態を示す機能ブロック図である。図1に示すように、本実施形態の認証管理システムは、ネットワーク60に相互に安全性をもって通信可能に接続された任意の数のコンピュータシステム10, 50、ネットワーク60上に相互に安全に通信可能に接続された任意の数の電子文章データ保管システム20、任意の数の認証データ保管システム30, 40を有している。

【0010】コンピュータシステム10, 50は、電子文章データ1を作成するワープロ機能、パスワードなど安全性を有した通信手段で電子文章データ1の送信や受信を実行する通信機能、認証データ3, 4の送信や受信を実行する認証機能、バーコード等のイメージデータを印字する出力機能を有する。

【0011】本実施形態の電子文章データ保管システム20は、電子文章データ保管工程を実行する手段であって、コンピュータ等を使用した電子文書を、この電子文書の文章承認者に対する認証の根拠と成り得る認証データ及びこの文章承認者に対する認証の根拠と成り得る認証データの管理番号とともに承認データの受付時の状態で保管し、電子文書に対する認証の根拠と成り得る電子文章管理番号に基づく認証データを追加した電子文章データ1を生成する。

【0012】換言すれば、電子文章データ保管システム

20は、認証手段としての印章及び/またはサインイメージの近傍であってこの印章及び/またはサインイメージの真贋の確認が容易な位置に、この印章及び/またはサインイメージに対する認証の根拠と成り得る管理番号及び/または使用番号3-3, 4-3をバーコード形式で付記するとともに、印字文書の中に文書の管理番号及び/または保管機関のコードをバーコード形式で付記して電子文書を保管する。

【0013】また電子文章データ保管システム20は、接続されたコンピュータシステム10, 50の特定されたユーザーから電子文章データ1を安全に送受信する機能、電子文章データ1を保管し、その電子文章データ1から必要な認証者を読み出し、通信手段を用いて認証者の承認を得て、認証データ保管システム30, 40から認証データ3, 4を受け取る機能を有する。

【0014】本実施形態の認証データ保管システム30, 40は、認証データ保管工程を実行する手段であって、個人や法人に対する認証の根拠と成り得る印章やサインなどのイメージデータを認証データとして保管し、この個人や法人からの要求に応じて、この要求のあった認証データ及びこの認証データに対する認証の根拠と成り得る管理番号を電子文章データ保管システム20に送付する。

【0015】換言すれば、認証データ保管システム30, 40は、個人及び/または法人に対する認証の根拠と成り得る印章やサインを含むイメージデータを認証データ3, 4として保管する。

【0016】このような電子文章データ保管システム20と認証データ保管システム30, 40とは、相互に認証データ3, 4の管理番号と文章管理番号を保管及び管理する。

【0017】また認証データ保管システム30, 40は、認証者から受け取った認証データ3, 4を保管管理するとともに、電子文章データ保管システム20との間でネットワーク60を介して取得する電子文章データ1からの認証データ要求に対応して、認証者のコンピュータシステム10, 50と通信手段により承認を取り、管理番号付きの認証データ3, 4を送付する機能を有する。

【0018】統いて、本実施形態の認証管理システムの動作を説明する。

【0019】コンピュータシステム10を用いて電子文章データ1を作成し、電子文章データ保管システム20に自らの承認データを添付して保管すると、この承認データの保管に応じて、電子文章データ保管システム20は、認証データ保管システム30, 40に必要認証者の認証データ3, 4を要求する。

【0020】この認証データ3, 4を要求に応じて、各認証データ保管システム30, 40は、電子文章データ保管システム20から文書データ管理番号を受け取って

仮保管し、各認証者の承認を得て、電子文章データ保管システム20に認証データ3、4と管理番号を送付する。

【0021】この認証データ3、4と管理番号の送付に応じて、認証データ保管システム30、40は、文書データ管理番号を保管する。

【0022】これに応じて、電子文章データ保管システム20は、各認証データ3、4を収集後、電子文書の中に認証データ3、4とその管理番号、電子文章データ保管システム20の管理番号を記入し、その管理番号をバーコードにて表示し、電子文章データ1として保管し、各認証者のコンピュータシステム10、50にその電子文章データ1を送信する。

【0023】この電子文章データ1の送信に応じて、受信した各コンピュータシステム10、50は、その電子文章データ1を保管、印字を行う。

【0024】次に、本実施形態の認証管理システムにおいて、図2に示す電子文章データ1が作成された過程について説明する。図2は、図1の認証管理システムで用いられる電子文章データ1の印字結果の概略構成を示している。

【0025】図2に示す電子文章データ1は、電子文章データ保管システム20に保管され、そのシステムを特定する管理番号とそのバーコード2、文書管理の文書番号とそのバーコード1-1、認証者の認証データ3、4を文書内に有している。また電子文章データ1には、文書名1-2の場所に題名が、文1-3の場所に文の内容が記載されるようになっている。

【0026】認証データ3は、認証イメージデータ3-1、認証データ保管システム30の管理番号と認証者の管理番号3-2、使用番号3-3、及びこれらの各々のバーコードを有している。

【0027】認証データ4は、認証イメージデータ4-1、認証データ保管システム40の管理番号と認証者の管理番号4-2、使用番号4-3、及びこれらの各々のバーコードを有している。

【0028】図3は、本発明の認証管理方法を用いた文書作成手順の一実施形態を示すフローチャートである。本実施形態の認証管理方法は、コンピュータ等を使用した電子文書の認証管理方法であって、コンピュータ等を使用した電子文書及び/または電子文書の印字結果に表示される認証としての印章及び/またはサインイメージに、この認証の根拠と成り得る管理番号及び/または使用番号をバーコード形式で付記する工程と、文書に対する認証の根拠と成り得る管理番号及び/または保管システムのコードをこの電子文書中にバーコード形式で付記する工程とを実行するために、電子文章データ保管工程、認証データ保管工程を有している。

【0029】電子文章データ保管工程は、図3に示すように、電子文章データ保管システム20が実行する工程

であって、コンピュータ等を使用した電子文書を、この電子文書の文章承認者に対する認証の根拠と成り得る認証データ及びこの文章承認者に対する認証の根拠と成り得る認証データの管理番号とともに承認データの受付時の状態で保管し、電子文書に対する認証の根拠と成り得る電子文章管理番号に基づく認証データを追加した電子文章データ1を生成する。

【0030】換言すれば、電子文章データ保管工程は、認証工程としての印章及び/またはサインイメージの近傍であってこの印章及び/またはサインイメージの真贋の確認が容易な位置に、この印章及び/またはサインイメージに対する認証の根拠と成り得る管理番号及び/または使用番号3-3、4-3をバーコード形式で付記するとともに、印字文書の中に文書の管理番号及び/または保管機関のコードをバーコード形式で付記して電子文書を保管する。

【0031】このような電子文章データ保管工程は、接続されたコンピュータシステム10、50の特定されたユーザーから電子文章データ1を安全に送受信する工程を有し、電子文章データ1を保管し、この電子文章データ1から必要な認証者を読み出し、通信工程を用いて認証者の承認を得て、認証データ保管工程から認証データ3、4を受け取る工程を有する。

【0032】一方、認証データ保管工程は、図3に示すように、認証データ保管システム30、40が実行する工程であって、個人や法人に対する認証の根拠と成り得る印章やサインなどのイメージデータを認証データとして保管し、この個人や法人からの要求に応じて、この要求のあった認証データ及びこの認証データに対する認証の根拠と成り得る管理番号を電子文章データ保管工程に送付する。

【0033】換言すれば、認証データ保管工程は、個人及び/または法人に対する認証の根拠と成り得る印章やサインを含むイメージデータを認証データ3、4として保管する。

【0034】このような電子文章データ保管工程と認証データ保管工程とは、相互に認証データ3、4の管理番号と文章管理番号を保管及び管理する。

【0035】このような認証データ保管工程は、認証者から受け取った認証データ3、4を保管管理する工程を有し、電子文章データ保管工程との間でネットワーク60を介して取得する電子文章データ1からの認証データ要求に対応して、認証者のコンピュータシステム10、50と通信工程とにより承認を取り、管理番号付きの認証データ3、4を送付する工程を有する。

【0036】次に、電子文章データ1の作成手順を図3を用いて説明する。電子文章データ1が図2に示す甲と乙の2人が承認する書類(契約書等を含む)の場合であって、認証者の一人である“甲”(図2、図3に示す”中山“氏)がコンピュータシステム10を使用して、電

子文章データ1を作成するケースについて説明する。

【0037】中山“氏が、コンピュータシステム10を使用して認証者の認証管理番号の付いた電子文章の仮データを作成する。ここで、仮データと称するのは、電子文章データ保管システム20の管理番号や文書番号、認証データ3, 4をまだ含んでいないからである。

【0038】コンピュータシステム10は、電子文章データ保管システム20にこの電子文章の仮データを送信するとともに、この電子文章データ保管システム20から文書管理番号を取得する。

【0039】電子文章データ保管システム20は、取得した文書管理番号を文書管理ファイル21に仮保管する。

【0040】電子文章データ保管システム20は、電子文章データ1中の必要な認証者の認証管理番号に基づいて、認証データ保管システム30、40の各々に認証データ3, 4を要求する。認証データ保管システム30、40の各々に認証データ3, 4を要求する場合、電子文章データ保管システム20は、システムの管理番号、文書管理番号、及び仮の電子文章データ1を送信する。

【0041】要求順序は、作成者の認証データ3, 4に基づいて求める。認証データ3, 4を要求された各認証データ保管システム30、40は、電子文章データ1の仮文書を添付して各認証者に承認を求める。

【0042】電子文章データ保管システム20は、認証データ保管システム30を通して“甲“に該当する”中山“氏の承認に応じて、認証データ保管システム30から認証データ3を入手し、認証データ保管システム40を介して“乙“に該当する”田中“氏の承認を得ることにより、認証データ保管システム40から認証データ4入手する。

【0043】各認証データ保管システム30, 40は、認証管理ファイル31, 41の各々に保管されている各々の認証者の管理番号に対応させて、使用番号3-3, 4-3、及び電子文章データ保管システム20の管理番号と文書の管理番号を関連づけて保管する。

【0044】認証データ3は、認証イメージデータ3-1、認証データ保管システム30の管理番号と認証者の管理番号3-2、使用番号3-3、及びこれらの各々のバーコードを有している。

【0045】認証データ4は、認証イメージデータ4-1、認証データ保管システム40の管理番号と認証者の管理番号4-2、使用番号4-3、及びこれらの各々のバーコードを有している。

【0046】電子文章データ保管システム20は、最終的な電子文章データ1を完成し、保護された状態で文書管理ファイル21に保管する。

【0047】この電子文章データ1の内容を確認することが許可された、特定の人もしくは一般の人はコンピュータシステム10, 50からこの電子文章データ保管シ

ステム20にアクセスすることにより、電子文章データ1を入手し、印字することが可能となる。

【0048】以上第1実施形態を要約すれば、認証としての印章及び／またはサインイメージの真質の確認が容易なように認証としての印章及び／またはサインイメージの近傍にその認証の根拠と成り得る管理番号及び／または使用番号3-3, 4-3を数字とバーコード形式で付記するとともに印字文書の中に文書の管理番号及び／または保管機関のコードを数字とバーコード形式で付記し、バーコードリーダーを持つコンピュータシステム10, 50にてチェックすることにより、迅速に認証データ3, 4や電子文章データ1を検索し、各保管システムから取り出すことができるようになる。その結果、電子文章データ1に含まれる、認証データ3, 4から容易に認証データ保管システム30, 40を割り出せ、アクセスすることにより認証データ3, 4の真質を容易に判定でき、また、電子文章データ1をも検索し易いというメリットを有する。

【0049】更に、認証データ3, 4を必要とする電子文章データ1を保管する電子文章データ保管システム20と個人及び／または法人に対する認証の根拠と成り得る印章やサインを含むイメージデータを認証データ3, 4として保管する認証データ保管システム30, 40を独立したシステムとして構成し、これをネットワーク60で認証者のコンピュータシステム10, 50と、及び、認証データ保管システム30, 40相互に接続することにより、電子文章データ1の作成者が、作成した仮の電子文章データ1を一旦、電子文章データ保管システム20に保管し、電子文章データ保管システム20が認証データ保管システム30, 40を介して認証データ3, 4を得るとともに相互に認証データ3, 4の管理番号と文書管理番号を保管及び管理することができるようになる。その結果、電子文章データ保管システム20と認証データ保管システム30, 40が各々、独立したシステムとなっており、安全性に富んだ、オープンなシステムを構成できるようになる。

【0050】(第2実施形態)本実施形態の認証管理システムは、電子文章の仮データの作成時に、作成者が自らの認証データ3, 4を認証データ保管システム30, 40から仮入手する。このとき、認証データ保管システム30, 40には、電子文章データ保管システム20の管理番号や文書番号は与えられず、認証データ3, 4の仮使用番号が送信される。

【0051】電子文章データ保管システム20に仮文章データが送信された後、作成者の承認を得ることなく、電子文章データ保管システム20と認証データ保管システム30, 40間で管理番号や文書番号の送信を行う。この場合、承認手続きが一部省力できるといったメリットを有する。

【0052】以上第2実施形態を要約すれば、認証とし

ての印章及び／またはサインイメージの真贋の確認が容易なように認証としての印章及び／またはサインイメージの近傍にその認証の根拠と成り得る管理番号及び／または使用番号3-3, 4-3を数字とバーコード形式で付記するとともに印字文書の中に文書の管理番号及び／または保管機関のコードを数字とバーコード形式で付記し、バーコードリーダーを持つコンピュータシステム10, 50にてチェックすることにより、迅速に認証データ3, 4や電子文章データ1を検索し、各保管システムから取り出すことができるようになる。その結果、電子文章データ1に含まれる認証データ3, 4から容易に認証データ保管システム30, 40を割り出せ、アクセスすることにより認証データ3, 4の真贋を容易に判定でき、また、電子文章データ1をも検索し易いというメリットを有する。

【0053】更に、認証データ3, 4を必要とする電子文章データ1を保管する電子文章データ保管システム20と個人及び／または法人に対する認証の根拠と成り得る印章やサインを含むイメージデータを認証データ3, 4として保管する認証データ保管システム30, 40を独立したシステムとして構成し、これをネットワーク60で認証者のコンピュータシステム10, 50と、及び、認証データ保管システム30, 40を相互に接続することにより、電子文章データ1の作成者が、作成した仮の電子文章データ1を一旦、電子文章データ保管システム20に保管し、電子文章データ保管システム20が認証データ保管システム30, 40を介して認証データ3, 4を得るとともに相互に認証データ3, 4の管理番号と文章管理番号を保管及び管理することができるようになる。その結果、電子文章データ保管システム20と認証データ保管システム30, 40が各々、独立したシステムとなっており、安全性に富んだ、オープンなシステムを構成できるようになる。

【0054】なお、本実施の形態においては、本発明は電子文章データに限定されず、本発明を適用する上で好適な電子マネー (Electronic Money, Digital Cash) に対する認証技術、クレジットカードに対する認証技術、電子商取引 (Electronic Commerce) に対する認証技術、電子銀行システム (Electronic Banking) に対する認証技術等に広く適用することができる。また、上記構成部材の数、位置、形状等は上記実施の形態に限定されず、本発明を実施する上で好適な数、位置、形状等にすることができる。また、各図において、同一構成要素には同一符号を付している。

【0055】

【発明の効果】本発明は、認証としての印章やサインイメージの真贋の確認が容易なように認証としての印章やサインイメージの近傍にその認証の管理番号及び使用番

号をバーコード形式で付記するとともに印字文書の中に文書の管理番号及び保管機関のコードをバーコード形式で付記し、オープン性に富みかつ信頼性の高い認証管理システム及び認証管理方法の実現のため電子文書を保管する電子文章データ保管システムと個人や法人の印章やサインなどのイメージデータを認証データとして保管する認証データ保管システムにおいて、相互に認証データの管理番号と文章管理番号を保管及び管理する。

【0056】これにより、電子文章データ保管システムと認証データ保管システムの両方の管理システムに通信的に接続されたコンピュータのバーコードリーダーを用いて認証データの下のバーコードを読みとることにより、認証データ保管システムからその文章データを承認したかどうかの確認が取れるようになる。また文章データの管理番号のバーコードを読みとり、電子文章データ保管システムからその文章が正しいことを確認できる。その結果、コンピュータ等を使用した電子文書及び電子文書の印字結果に表示される認証としての印章やサインイメージの真贋の確認が容易な印字及び表示ができるようになり、セキュリティ性の向上を図ることができるといった効果を奏する。

【0057】また、認証データに管理番号のバーコードを追加することにより、電子文書及び電子文書の印字結果に表示される認証としての印章やサインイメージの真贋の確認が容易になるといった効果を奏する。

【0058】更に、認証データと文章データに管理番号を付けるとともに相互に保管管理することにより、認証データと電子文書を各々別々にかつ関連づけて確認容易な形態で保管できるようになる。その結果、高いオープン性との高い信頼性とを両立できるといった効果を奏する。

【図面の簡単な説明】

【図1】本発明の認証管理システムの一実施形態を示す機能ブロック図である。

【図2】図1の認証管理システムで用いられる電子文章データの印字結果の概略構成を示している。

【図3】本発明の認証管理方法を用いた文書作成手順の一実施形態を示すフローチャートである。

【符号の説明】

1…電子文章データ

1-1…文書管理の文書番号とそのバーコード

1-2…文書名

1-3…文

2…管理番号とそのバーコード

3, 4…認証者の認証データ

3-1, 4-1…認証イメージデータ

3-2, 4-2…管理番号と認証者の管理番号

3-3, 4-3…使用番号

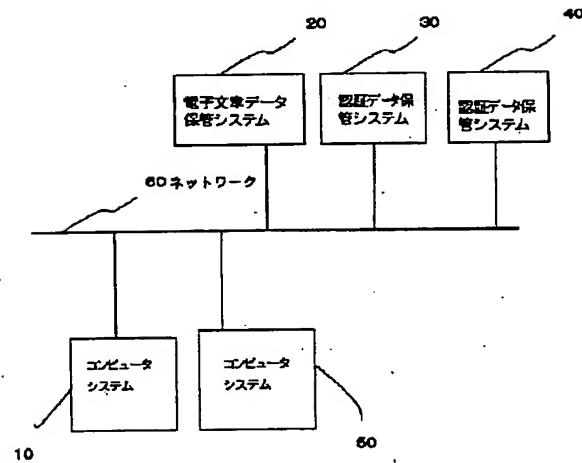
10, 50…コンピュータシステム

20…電子文章データ保管システム

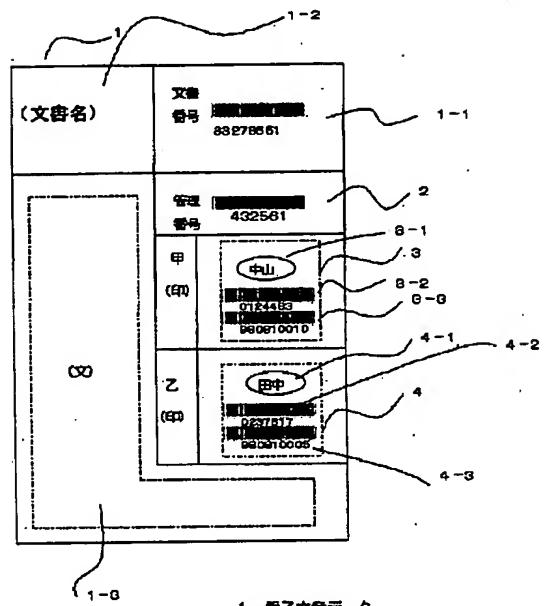
21…文書管理ファイル
30, 40…認証データ保管システム

31, 41…認証管理ファイル
60…ネットワーク

【図1】



【図2】



1...電子文書データ
1-1...文書管理の文書番号とそのバーコード
1-2...文書名
1-3...文
2...管理番号とそのバーコード
3, 4...認証者の認証データ
3-1, 4-1...認証イメージデータ
3-2, 4-2...管理番号と認証者の管理番号
3-3, 4-3...使用番号

【図3】

